Data Protection Policy

This Policy outlines the responsibilities of Stratworth University ("the Company") concerning data protection and the rights of customers, learners and business contacts ("data subjects") concerning their personal data under the Data Protection Act 2018 (formally EU Regulation 2016/679 General Data Protection Regulation ("GDPR")).

Core Definitions

- Personal Data: Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- Processing: Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Policy Statement

The Company is committed to complying with the Data Protection Act 2018 and upholding the principles of lawful, fair, and transparent processing of personal data. We respect the legal rights, privacy, and trust of all individuals with whom we deal.

Principles Underlying Our Data Processing Policy and Procedures

The Company adheres to the following data protection principles:

- Lawfulness, Fairness, and Transparency: Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Purpose Limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Data Minimization: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accuracy: Personal data must be accurate and, where necessary, kept up to date.
- Storage Limitation: Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures.

Rights of Data Subjects

The Data Protection Act 2018 grants data subjects the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object
- Rights with respect to automated decision-making and profiling

Lawful, Fair, and Transparent Processing

The Data Protection Act 2018 requires lawful, fair, and transparent processing of personal data without adversely affecting the rights of the data subject. Processing is lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.

- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them.
- The processing is necessary for compliance with a legal obligation to which the controller is subject.
- The processing is necessary to protect the vital interests of the data subject or of another natural person.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

For "special category data" (sensitive personal data), additional conditions must be met for lawful processing.

Specified, Explicit, and Legitimate Purposes

The Company collects and processes personal data for specific purposes outlined in this Policy or expressly permitted by the Data Protection Act 2018. Data subjects are informed of the purposes for which the Company uses their personal data.

Adequate, Relevant, and Limited Data Processing

The Company only collects and processes personal data for the specific purpose(s) of which data subjects have been informed.

Accuracy and Keeping Data Up-to-Date

The Company ensures all personal data collected, processed, and held is accurate and up-to-date. This includes rectification of personal data at the request of a data subject. Regularly checking data accuracy is essential.

Data Retention

- Limited Retention: The Company will not retain personal data for longer than necessary in light of the purpose(s) for which it was originally collected, held, and processed.

- Deletion Upon Completion: When personal data is no longer required for its original purpose(s), all reasonable steps will be taken to erase or otherwise dispose of it securely and without delay.
- Detailed Retention Policy: For comprehensive information on the Company's data retention approach, including specific retention periods for various personal data types, please refer to our separate Data Retention Policy.

Secure Processing

- Data Security Commitment: The Company is committed to ensuring that all collected, held, and processed personal data is kept secure and protected against unauthorized or unlawful processing, accidental loss, destruction, or damage. Technical and organizational measures to achieve this are outlined later in this Policy.

Accountability and Record-Keeping

- Data Protection Officer: Stratworth University has appointed Amarachi Peace Ekwealor as its Data Protection Officer. You can contact Ms. Ekwealor by email at amara@stratwortuniversity.org.
- Data Protection Oversight: The Data Protection Officer is responsible for overseeing the implementation and monitoring compliance with this Policy, other data protection-related policies of the Company, and the Data Protection Act 2018 and other applicable data protection legislation.
- Internal Records: The Company maintains written internal records of all personal data collection, holding, and processing activities. These records contain the following information:
    - Details of the Company, its Data Protection Officer, and any relevant third-party data processors engaged.
    - The purposes for which the Company collects, holds, and processes personal data.
    - Categories of personal data collected, held, and processed by the Company, and the categories of data subjects to which that data pertains.
    - Details of any personal data transfers to non-EEA countries, including security safeguards implemented.
    - Data retention periods for different personal data types.
    - Detailed descriptions of all technical and organizational measures taken to ensure data security.

Data Protection Impact Assessments

- New Projects and Uses of Data: The Company will conduct Data Protection Impact Assessments for any new projects and/or new uses of personal data.
- DPIA Content and Oversight: Data Protection Impact Assessments are overseen by the Data Protection Officer and address the following aspects:
    1. Types of personal data to be collected, held, and processed.
    2. Purposes for which personal data will be used.
    3. The Company's objectives.
    4. How personal data will be used.
    5. Internal and/or external parties to be consulted.
    6. Necessity and proportionality of data processing in relation to the intended purpose(s).
    7. Risks posed to data subjects.
    8. Risks posed both within and to the Company.
    9. Proposed measures to minimize and address identified risks.

Keeping Data Subjects Informed

- Transparency Regarding Data Use: The Company is committed to providing data subjects with the information outlined below:
    - Direct Data Collection: Data subjects will be informed of the purpose of data collection at the time of collection if data is obtained directly from them.
    - Indirect Data Collection: For personal data obtained from a third party, relevant data subjects will be informed of the purpose for its use:
        - When the data is used to communicate with the data subject, during the first communication.
        - Before the data is transferred to another party, if applicable.
        - As soon as reasonably possible, but no later than one month after the data is obtained.
- Information Provided to Data Subjects: The following information will be provided:
    - Company details, including the Data Protection Officer's contact information.
    - Purposes for which personal data is being collected and processed (as detailed in this Policy) and the legal basis justifying that collection and processing.
    - Any legitimate interests justifying the Company's collection and processing of personal data (if applicable).
    - Categories of personal data collected and processed, for situations where data is not obtained directly from the data subject.
    - Details of any third parties to whom personal data will be transferred (if applicable).

    - Details of any transfer of personal data to a third party located outside the European Economic Area (EEA), including safeguards implemented.
    - Data retention details.
    - Information on the data subject's rights under the Data Protection Act 2018.
    - Information on the data subject's right to withdraw consent for the Company's processing of their personal data at any time.
    - Information on the data subject's right to complain to the Information Commissioner's Office

Data Subject Access

- Subject Access Requests (SARs): Data subjects have the right to submit Subject Access Requests ("SARs") at any time to learn more about the personal data the Company holds about them, the purpose of such data collection and processing, and the justification for it.
- Submitting SARs: SARs can be submitted in writing using the Company's Subject Access Request Form or any other written communication. Requests should be addressed to the Data Protection Officer at Stratworth University, Stratworth Group LLC 30 N Gould STE 4000, Sheridan WY 82801. You can also submit an SAR by email at amara@stratworthuniversity.org.
- Response Time: The Company typically responds to SARs within one month of receipt. However, this timeframe can be extended by up to two months for complex requests or a high volume of requests. The data subject will be informed if additional time is needed.
- SAR Processing: All SARs are handled by the Company's Data Protection Officer.
- Fees: The Company does not charge a fee for handling standard SARs. However, the Company reserves the right to charge reasonable fees for:
    - Providing additional copies of information already provided to a data subject.
    - Requests that are manifestly unfounded or excessive, particularly repetitive requests.

Rectification of Personal Data

- Right to Rectification: Data subjects have the right to request the Company to correct any inaccurate or incomplete personal data they hold.
- Processing Time: The Company will rectify the data in question and inform the data subject within one month of the request. This period can be extended by up

to two months for complex requests. The data subject will be informed if additional time is needed.
- Informing Third Parties: If any affected personal data has been disclosed to third parties, the Company will notify them of any necessary rectification.

Erasure of Personal Data

Data subjects have the right to request that the Company erase their personal data under the following circumstances:

- The data is no longer necessary for the original purpose(s) of collection or processing.
- The data subject withdraws consent for the Company to hold and process their data.
- The data subject objects to the Company holding and processing their data (and there is no overriding legitimate interest for the Company to continue doing so).
- The data has been processed unlawfully.
- The data needs to be erased for the Company to comply with a legal obligation.

Unless the Company has a legitimate reason to refuse erasure, all requests will be fulfilled, and the data subject informed within one month of the request. This period can be extended by up to two months for complex requests. The data subject will be informed if additional time is needed.

In the event that personal data must be erased in response to a data subject's request and has been disclosed to third parties, those parties will be informed of the erasure (unless it is impossible or requires disproportionate effort).

Restriction of Personal Data Processing

Data subjects have the right to request that the Company restrict the processing of their personal data. If a data subject makes such a request, the Company will only retain the minimum amount of personal data necessary to ensure it is not further processed.

In the event that any affected personal data has been disclosed to third parties, those parties will be informed of the applicable restrictions on processing it (unless it is impossible or requires disproportionate effort).

Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

- Objection Based on Legitimate Interests: If a data subject objects based on legitimate interests, the Company will cease processing unless it can demonstrate compelling legitimate grounds for processing that override the data subject's interests, rights, and freedoms, or the processing is necessary for legal claims.
- Objection to Direct Marketing: If a data subject objects to processing for direct marketing, the Company will cease such processing immediately.
- Objection to Research or Statistics: If a data subject objects to processing for scientific and/or historical research and statistics purposes, they must demonstrate grounds relating to their particular situation under the Data Protection Act 2018. The Company is not required to comply if the research is necessary for the public interest.

Personal Data and Security

Personal Data Collected

The Company collects, holds, and processes the following personal data:

- Contact Information: This includes names, phone numbers, email addresses, and qualifications.

Data Security

The Company implements robust security measures to protect personal data:

Data Transfer and Communication

- Encryption: All emails containing personal data are encrypted using specialized software.
- Confidentiality: Emails containing personal data are marked "confidential."
- Secure Networks: Personal data is transmitted only over secure networks. Transmission over unsecured networks is strictly prohibited.
- Wireless Network Restrictions: Personal data is not transmitted over wireless networks unless there's no viable wired alternative.
- Secure Email Handling: Personal data from emails is copied and stored securely. The original emails are then deleted, along with any associated temporary files.

- Fax Transmission: When sending personal data via fax, recipients are informed in advance and are ready to receive the transmission.
- Hardcopy Transfers: Hardcopy personal data is either delivered directly to the recipient or sent via secure postal services like Royal Mail Registered or 1st/2nd Class Signed For.
- Physical Transfers: Personal data transferred physically (hardcopy or electronic media) is securely packaged in a container marked "confidential."

Data Storage

- Secure Electronic Storage: Electronic personal data is stored securely using passwords and data encryption.
- Secure Physical Storage: Hardcopy personal data and electronic copies on physical media are stored securely in locked storage containers.
- Regular Backups: Electronic personal data is backed up daily and stored securely onsite. Backups are also encrypted.
- Mobile Device Restrictions: Personal data is not stored on mobile devices (laptops, tablets, smartphones) without the Data Protection Officer's explicit written approval. Any approved storage must adhere to strict guidelines and time limits.
- Device Restrictions: Personal data is not transferred to personally owned devices. Transfers to devices owned by agents, contractors, or other parties are only allowed if those parties agree to comply fully with the Data Protection Act 2018 and this Policy, including demonstrating appropriate technical and organizational measures.

Data Disposal

When personal data is no longer needed, it is securely deleted and disposed of, including any copies.

Data Security: Usage and IT Security

Data Usage

- Restricted Access: Personal data will only be accessed by employees, agents, contractors, or other authorized parties who require it to perform their specific duties.
- Formal Access Requests: Any employee, agent, contractor, or other party who needs access to personal data they don't already have must formally request it from the Data Protection Officer.

- Authorized Transfers Only: Personal data will not be transferred to any unauthorized individuals or entities. Transfers must be authorized by the Data Protection Officer.
- Secure Handling: Personal data must be handled with care at all times. It should never be left unattended or visible to unauthorized individuals.
- Secure Workstations: When leaving a workstation with personal data displayed, users must lock both the computer and screen.
- Marketing Consent: When using personal data for marketing purposes, Gabrielle Stirling will ensure that appropriate consent has been obtained and that no data subjects have opted out, either directly or through third-party services like the TPS.

IT Security

- Strong Password Practices: Passwords used to protect personal data must be strong, changed regularly, and should not be easily guessed. They must contain a combination of uppercase and lowercase letters, numbers, and symbols.
- Password Security: Passwords should never be written down or shared with others. Forgotten passwords must be reset using the appropriate procedures. IT staff do not have access to user passwords.
- Software Updates: All software (applications and operating systems) must be kept up-to-date. The Company's IT staff is responsible for installing security updates promptly, unless there are valid technical reasons not to do so.
- Software Installation Control: No software can be installed on Company-owned computers or devices without prior approval from the Company.

Organizational Measures

The Company implements the following organizational measures to ensure the secure and responsible handling of personal data:

- Employee Awareness and Training: All employees, agents, contractors, and other authorized parties are made aware of their individual responsibilities and the Company's obligations under the Data Protection Act 2018 and this Policy. They receive training on data protection principles and practices.
- Need-to-Know Access: Only employees, agents, contractors, or other authorized parties who require access to personal data for their specific duties are granted access.
- Appropriate Supervision: Employees, agents, contractors, and other authorized parties who handle personal data are subject to appropriate supervision.
- Confidentiality and Discretion: Employees, agents, contractors, and other authorized parties are required to exercise care, caution, and discretion when

discussing work-related matters involving personal data, both within and outside the workplace.

- Regular Review and Evaluation: The Company regularly reviews and evaluates its methods of collecting, holding, and processing personal data.
- Data Retention Review: Personal data held by the Company is reviewed periodically, as outlined in the Data Retention Policy.
- Performance Evaluation: The performance of employees, agents, contractors, and other authorized parties handling personal data is regularly evaluated and reviewed.
- Contractual Obligations: All employees, agents, contractors, and other authorized parties are contractually bound to comply with the principles of the Data Protection Act 2018 and this Policy.
- Third-Party Obligations: Third-party agents, contractors, or other parties handling personal data on behalf of the Company must ensure that their employees involved in data processing adhere to the same standards as the Company's employees.
- Indemnification: Third-party agents, contractors, or other parties handling personal data are responsible for indemnifying the Company against any costs, liabilities, damages, losses, claims, or proceedings arising from their failure to comply with their obligations under this Policy.

International Data Transfers and Data Breach Notification

International Data Transfers

The Company may occasionally transfer personal data to countries outside the European Economic Area (EEA). Such transfers will only occur under one or more of the following circumstances:

- Adequate Level of Protection: The transfer is to a country or territory recognized by the European Commission as providing an adequate level of data protection.
- Appropriate Safeguards: The transfer is to a country or international organization that offers appropriate safeguards in the form of legally binding agreements, binding corporate rules, standard data protection clauses adopted by the European Commission, or other approved mechanisms.
- Informed Consent: The transfer is made with the informed consent of the relevant data subject(s).
- Contractual Necessity: The transfer is necessary for the performance of a contract between the data subject and the Company or for pre-contractual steps.
- Public Interest: The transfer is necessary for important public interest reasons.
- Legal Claims: The transfer is necessary for the conduct of legal claims.

- Vital Interests: The transfer is necessary to protect the vital interests of the data subject or another individual where the data subject is unable to give consent.
- Public Registers: The transfer is from a public register intended to provide information to the public.

Data Breach Notification

- Immediate Reporting: All personal data breaches must be reported immediately to the Company's Data Protection Officer.
- Notification to Supervisory Authority: If a data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must inform the Information Commissioner's Office without delay, and within 72 hours of becoming aware of the breach.
- Notification to Data Subjects: In cases where a data breach poses a high risk to data subjects' rights and freedoms, the Data Protection Officer must directly inform all affected data subjects without undue delay.
- Notification Content: Data breach notifications must include the following information:
    - Categories and approximate number of data subjects affected
    - Categories and approximate number of personal data records affected
    - Name and contact details of the Company's Data Protection Officer or other relevant contact point
    - Potential consequences of the breach
    - Details of steps taken or planned to address the breach, including measures to mitigate potential adverse effects

This policy has been reviewed, approved & authorized by:

Name: Prof. Dr. Lawrence Emeagwali

Position: Company Director

Date: December, 2024

Policy Review Date: December, 2027